# Prepare for the worst, hope for the best

JustCoding.com - August 06, 2008

*Draft a disaster recovery plan and keep it up to date*

Most health information management (HIM) directors think a disaster will never occur at their hospitals. And although channeling positive thoughts is generally laudable, it isn't a realistic approach when disaster can strike at any moment. A disaster doesn't necessarily need to take the form of a hurricane, tornado, or pandemic to severely incapacitate an HIM department. What happens when the power goes out? Or how about when the computer system crashes?

**Glennda Gore, RHIA,** vice president of risk management and chief compliance officer at McAlester (OK) Regional Health Center knows all too well the havoc that can ensue in HIM departments in the wake of a disaster. During January 2007, the town of McAlester experienced a severe ice storm. The weight of the ice caused power lines and telephone poles to snap and break, resulting in a power outage that lasted nearly two weeks. The hospital was able to function with a backup generator for the first two days, but when it failed unexpectedly, the hospital was without power for 45 minutes.

"We had surgeries going on, a C-section, and people under anesthesia," says Gore. "The whole hospital [staff] were running around with flashlights trying to assist physicians and patients. It was chaotic."

The hospital could not access its electronic records. Worse, the HIM department did not have a functioning computer because the facility had only factored in essentials, such as life support, when deciding which equipment should remain on the generator.

But the flow of patients into the emergency room (ER) continued, and Gore had to find a way to keep the department functioning.

Assistance from off-site transcriptionists and other hospitals helped pick up the slack, and this enabled McAlester staff members to get caught up on their workload. "We gave them [the offsite workers] access to the computer system, got HIPAA forms signed, they logged in, and they were immediately contract employees who helped us transcribe," says Gore.

Since the disaster, the hospital has made sure that at least one computer in the HIM department is connected to the generator, says Gore. This will ensure that electronic records are accessible, that a transcriptionist can function, and that physicians don't need to handwrite notes.

The HIM department also prints its master patient index every month and maintains a manual log of all new admissions, says Gore. "That way, if the ER calls and needs old records, we can go through our three-ring binder and see what the medical record number is," she says.

Keeping flashlights on hand is another good idea, says Gore. Most HIM departments are in the windowless depths of the hospital, and this makes functioning nearly impossible during power outages.

**Understand the requirements, rationale**

Anticipating and addressing the details associated with all types of potential disasters is necessary when drafting functional disaster recovery and emergency mode operations plans, says **Chris Apgar, CISSP,** president of Apgar & Associates, LLC, in Portland, OR. A disaster recovery plan outlines what to do in an emergency or a disaster and the necessary steps for recovery. An emergency mode operations plan provides a clear, step-by-step explanation of how to perform critical functions during the emergency or disaster.

"In the HIM department, the primary focus is going to be on having the data available when it's needed and where it's needed, and that is an important part of an emergency mode operations plan," Apgar says.

Data availability not only helps ensure patient safety during emergencies and disasters, it's also a Joint Commission (formerly JCAHO) and HIPAA requirement.

The Joint Commission requires hospitals to have a business continuity/disaster recovery plan for their information systems in information management (IM) 2.30. This standard requires the following:

- Plans for scheduled and unscheduled interruptions (including end-user training with downtime procedures)
- Contingency plans for operational interruptions, including hardware, software, or other systems failure
- Plans for minimal interruptions due to scheduled downtime
- An emergency service plan
- A backup system (electronic or manual)
- Data retrieval plans

IM.2.30 also requires hospitals to test their plans periodically to ensure that backup techniques work and that staff members implement the plan during emergencies.

Pursuant to 45 *Code of Federal Regulations (CFR)* 164.308 (a)(7), HIPAA also requires hospitals to plan for disasters. This provision of the *CFR* requires that hospitals have a data backup plan, a disaster recovery plan, and an emergency mode operations plan.

Testing these procedures and performing an application and data criticality analysis is wise, says Apgar.

The HIPAA security rule lists these requirements as "addressable." However, "addressable" isn't synonymous with "optional," says Apgar. "Addressable" means that hospitals must follow the requirements of the rule, adopt a process or practice that provides the same protections as the rule, or have a very good and documented reason not to adhere to the rule. Cost cannot be the sole reason for failure to adhere to an applicable rule.

**Perform a thorough systems inventory**

Understanding these requirements is the first step in creating a sound disaster recovery plan, and it can also help you avoid becoming the target of a CMS security audit, says Apgar. "CMS has indicated that its audit criteria are the entire security rule. So they're going to be looking at whether you have disaster recovery and emergency mode operations plans in place and whether they are up to date," he says.

But even the most thorough disaster recovery plan will not cross every "t" and dot every "i," Apgar adds. The unanticipated is always a possibility. This illustrates the importance of performing a detailed inventory that includes everything a disaster could affect. "This is the most onerous part of disaster recovery plan development," he says.

Conducting an inventory requires performing a thorough review of the following:

- All hardware, including biomedical devices, life support, and other equipment for critical procedures
- All software (i.e., systems that contain clinical patient information), people (i.e., those who need to access patient information to keep the business running), and data (i.e., location and backup procedures)

Assisting with the maintenance of this inventory may be a daunting task for HIM directors. Apgar suggests delegating oversight for portions of the inventory to the individual who has direct operational responsibility for that area of the hospital. "You end up with a far better plan, and it's a lot less disruptive of the business," he says.

**Disseminate, educate, and test**

Consider the following additional suggestions when drafting and testing your disaster recovery and emergency mode operations plans:

- Disseminate the plans to those individuals who have primary responsibilities in the disaster recovery or emergency mode operations plan. Ask all of them to keep copies of the plans at home.
- Test components of the plans even if a full test is impossible. For example, periodically test your generator to ensure that it's operable.
- Update the plans quarterly or more frequently as needed and as contacts change. This is the most difficult aspect to manage, says Apgar. "The problem with disaster recovery and emergency mode plans is that if you're not diligent, they become outdated very quickly," he says. "Your operations change, your people move around, [and] you buy new things."

*This article is adapted from the July issue of* ***Medical Records Briefing. For more information, click here***.